The Policies and the Realities of CIM - Lessons Learned

I am most grateful to the leadership of AFCEA for this opportunity to report about the Corporate Information Management program. Let me begin my remarks by a quotation, adapted from St. Augustine:

How is a wall more than a collection of bricks?
How is a church more than a collection of walls?
How is a faith more than a collection of churches?
How is what people do more than their faith?

My outline today will concentrate on faith and doing rather than on the equivalents of bricks, walls. It is only through a continuous reaffirmation of faith that any massive effort, such as CIM, may preserve its legitimacy.

In these remarks I want to establish that *Corporate Information Management* [CIM] is now an established doctrine, which is independent of Atwood, Andrews, Strassmann. Thousands are acting out its principles. CIM should not be seen as anything new. CIM is a revival of the initial intent of the leadership that defined *Information Resources Management* in the late 1960's as a way to manage information in the Federal government. CIM is not a solution to problems that are unique to Defense.

I am here to suggest that CIM principles, policies, guidelines and practices offer a legitimate, managerially sound and technologically advanced framework for information management for any diversified enterprise that is open to public scrutiny, whether from Congress or from its shareholders. Therefore, the talk today will concentrate on "lessons learned". I hope that the entire information management community will accept my interpretation of events as something that deserves further examination. My only claim to authority to talk about CIM derives from my presence in the CIM councils since its origins late in 1989 until two weeks ago. The sequence of this presentation will be historical. My premise is that those who do not wish to learn from history are doomed to repeat it, instead of progressing further.

The Origins of CIM

Without Inspired Leadership , Understanding and Power there is no Reform

Without Donald Atwood, the Deputy Secretary of Defense, there would be no CIM. Mr Atwood arrived in DoD with a thorough understanding of how information management is inseparable from general management. From his recent experiences, as Vice-Chairman and

senior Operating Group Executive of the General Motors Corporation, he came to realize that information management is a strategic tool for achieving major improvements in business. What is perhaps not known is that Mr. Atwood was one of the key negotiators between GM and EDS during and after the acquisition of EDS. I became involved with Mr. Atwood's immediate staff, as a consultant, after EDS took over all of GM's information assets in a precipitous coup that initially inflicted much damage to GM's competitive capabilities.

My exposure to GM sharpened my appreciation why Mr. Atwood wished to use information management strategically as a means for achieving cost reductions, as a tool for modernization, as an opportunity to create a commercial-like relationship between information providers and customers and as a means of streamlining DoD. Mr. Atwood understood the importance of a sound, deliberate, well planned, participatory and non-destructive approach to effecting organizational change through information technologies. His immediate, direct and personal involvement in steering CIM directions was always informed, consistent and unwavering. He always made the time available to discuss CIM progress and considers CIM as one of the major accomplishment during his term in office.

In July of 1989 Mr. Atwood and Mr. Cheney, launched the Defense Management Report (DMRD) which will influence whatever else would happen to CIM afterwards. The DMRD process would be responsive to the President's direction to "realize substantial improvements...in defense management overall." The DMRD's would establish policies and directions to improve defense capabilities under conditions of lower budgets. The initial DMRD statement clearly signaled that improvements in information management were to be one of the centerpieces of what the President and the Secretary of Defense wished to accomplish. The Comptroller had identified about $6 billion, or roughly 9% of total projected DMRD savings, over a seven year period, to come from cuts in information technologies. These savings would be realized through consolidations of data centers and applications. However, over half of the remaining 91% DMRD savings would require substantial further improvements in the information management. Thus the objectives for CIM were set as being central to further progress in Defense management.

Lesson #1: The lessons of the origins of CIM are equally applicable to all strategic uses of information technologies. It requires inspired leadership. It calls for top executive involvement. It must rely on financial targets. It calls for power and process to implement. Without these ingredients information management program are either aborted or born with chronic defects. In the presence of major genetic defects the best a baby can hope for is life as a crippled orphan and then as destitute adult. Therefore, the conception, the origin and the parenthood of any information management program shapes its prospects more than any other single influence.

Early CIM Start-up Attempts

You Cannot Reform an Organization by First Altering its Computers

The responsibility for the implementation of the information technology-related DMRD's were in the hands of the Comptroller's chain of command. The Comptroller was the designated IRM [Information Resource Management] Official, by law. The IRM oversight staff had always

reported to the Comptroller, so far as anyone could remember. There were comptroller executives who wished to use the consolidation of data centers and of applications as a means for accelerating the delivery of all DMRD projects.

Two task forces were put to work. One recommended to end the proliferation of over 10,000 mainframe computers at more than 1,000 locations by moving the mainframes to just a handful of central sites. The entire schema was inspired by the need to achieve quick operating cost reductions. The proposal looked to rapid physical consolidation as the source of savings. The proposal did not offer a network design, it neglected to consider the role of distributed computing, it did not have a credible concept of operations, it did not show how to organize and manage a $2 billion/year operation and it did not show how corralling obsolete mainframes into a few centers would avoid the likelihood of a monumental collapse. By the end of 1990 the proposals of the data center consolidation task force were rejected as not executable.

The second task force had the ambitious objectives to come up with single application solutions for every major business function. The new application would replace an enormous proliferation of identical applications. The leadership of the applications task force was delegated four levels below the Comptroller. This task force cloned itself into eight functional teams. At one time in 1990 there were over two hundred people DoD systems people on travel status, plus innumerable consultants, occupying conference rooms in the vicinity of the Pentagon. The teams were asked to follow an as yet untested process based on an off-the-shelf CASE (Computer Aided Software Engineering) tool. Dozens of sub-committees sat in conference rooms trying to conceive "open-systems, integrated data bases, client-server, machine independent, portable, high-level language applications" applications. The new applications would replace the existing accumulation of several hundred million lines of mostly undocumented code, running in just about every conceivable computing environment. The application task forces did not include a concern about benefits in their work. They did not support the proposed investments with any economic rationale. Even the most optimistic delivery dates for replacement systems extended into the 21st century. How to deliver DMRD cost reduction objectives between 1990 and 1997 was never explained. Early in 1991 the proposals of the applications consolidation task force were rejected as not executable.

The methodologies, processes and people who participated in these early start-up efforts reflected that traditional "grand design" approach to systems work. It was of the IRM people, by IRMs and largely for satisfying what IRM specialists usually worry about. It was an attempt to launch a much needed system modernization effort, but without the benefit of an explicit business improvement process or a structure to execute it. There was no policy, no technology framework, no business model no concept of operations. It was an attempt to re-impose system uniformity by placing reliance primarily on central IRM staffs to become agents of change at a time when the power of the central computing establishment was already eroding. The task force presentations covered computer applications, not Defense issues and solutions. The concerns of the presenters was indistinguishable from what I would get from computer specialists at Sears American Express, Shell Oil or General Foods. The ideas were 1960's mainframe vintage re bottled for the 1990's buzzwords. Considering the duplication, redundancy, proliferation and general chaos of information systems, the initial consolidation concepts had the support from th

Congress and the Comptroller. The situation cried for a radical change. Congress obliged. It cut the Services' systems development budgets severely and transferred about a quarter of what remained to the Comptroller for use as a lever to encourage consolidations.

Lesson #2: There are lessons to be learned from the early CIM start-up attempts. Apply financial incentives and do detailed technology planning but only after you have laid out a plan how the pieces fit together. Policy must always lead. Business methods come always ahead. Never engage without measures of performance. Build models before your consider looking at systems and applications. Never but never make decisions about applications, computing and telecommunications until you have experienced managers, proven organizations, top level policies, generally accepted measures and conceptual models of operation in place. Make sure that you have an organization that is commensurate with the task. Do not expect enthusiastic amateurs do a job that often kills even experienced professionals.

Laying Foundations: The Executive Level Group Report

If you want to make major improvements you should first ask outsiders.

Sometime in November of 1989 I received a call from David Hill, the Chief Information Executive of General Motors. Would I join a newly created Department of Defense Federal Advisory Board for Information Management to provide guidelines how to implement CIM? The Board, also known subsequently as the Executive Level Group [ELG] would report to Mr. Atwood. Appointing an outside Board made sense. If you want to make major changes in an organization that has deep roots sunk into tradition, you must bring in outsiders. Such outsiders must have a broad perspective. They must had prior experience in doing organizational surgery. The ELG group met such qualifications.

The ELG met for six months. We examined how the elements of a $9.2 billion annual IRM budget were put together. What we found was neither pretty, economical nor it made much sense. There was a leadership, policy and technology vacuum at the top. The world's largest information processing organization looked more like a vast field of custom-crafted shanties than an organized and interoperable enterprise.

In September 1990 the ELG delivered to the Secretary of Defense a plan on CIM directions. The basic idea of the ELG report was that if you want to have an integrated war-support capability, you need an integrated information strategy. The report spelled out what policies were necessary to obtain coordinated capabilities. The Services signed up to the ELG recommendations, since the policies were sufficiently general not to appear as requiring immediate changes. The Services also secured an agreement that any further efforts towards OSD-level data center consolidations would be stopped. Instead, Mr. Atwood agreed to proceeding with Service-managed consolidations, within existing organizations. The Services (and the Defense Logistics Agency) agreed to deliver a large share of what the Comptroller had originally estimated as savings.

The principles of the ELG are as good today as when they were conceived. They are common sense, generic and apply to any large organization that requires operational interdependency:

- Information will be managed through centralized control and decentralized execution.
- Simplification by elimination and integration is to be preferred to automation whether developing new or enhancing existing information systems.
- Proposed and existing business methods will be subject routinely to cost-benefit analysis which includes benchmarking against the best public and private sector achievement.
- New business methods shall be proven or validated before implementation.
- Information systems performing the same function must be common unless specific analysis determines they should be unique.
- Functional management shall be held accountable for all benefits and all directly controllable costs of developing and operating their information systems.
- Information systems shall be developed and enhanced according to a Department-wide methodology and accomplished in a compressed time-frame in order to minimize the cost of development and achieve early realization of benefits.
- Information systems shall be developed and enhanced in the context of process models that document business methods.
- The computing and communications infrastructure shall be transparent to the information systems that rely upon it.
- Common definitions and standards for data shall exist DoD-wide.
- Wherever practicable, information services shall be acquired through competitive bidding considering internal and external sources.
- Data must be entered only once.
- Access to information shall be facilitated, and/or controlled and limited, as required. Information must also be safeguarded against unintentional or unauthorized alteration, destruction, or disclosure.
- The presentation between the user and system shall be friendly and consistent.

During my many visits I became concerned about the isolation of the $9.2 billion "IRM" establishment as run by the Comptroller. The IRM bias, buttressed by OMB, GAO and GSA regulations, focused entirely on "back office" automation such as in finance, personnel, medical materials and logistics. The "customer end" of Defense, which is in Command, Control Communications and Intelligence [C3I] – estimated to be at least three time larger than IRM - was run as if it were on a separate continent. There were stake-holders that made sure that it stayed that way, although there was a notable exception. The Army had already started a transition that would conceptually, organizationally and technically eliminate the damaging barriers between the "back office" and the "customer end" of Defense.

Every text book on information management asserts that unless you proceed with the design of systems starting from the "customer end" inwards to the "back office", you will end up with a defective design. The charter of the ELG was nevertheless clear: concentrate on the "back

office", do not touch C3I and make sure that finance and accounting remain the priority. The ELG did not make recommendations of how the Department should organize for CIM.

Events overtook my concerns about the insupportable barriers that split all Defense between business systems and command, control, communications and intelligence. In November Mr. Cheney announced that the Assistant Secretary of Defense for C3I, Mr. Duane Andrews, would become responsible for overall information management. By February 1991, Mr. Andrews put in place all of the fundamental elements that would henceforth shape CIM:

- enlarged the charter of the Defense Communications Agency to cover all information services, as the Defense Information Systems Agency [DISA];
- created within DISA a well-funded CIM support organization under the direction of Mr. Denis Brown;
- appointed me as Director of Defense Information, and Principal Deputy Assistant Secretary;
- delegated the authority for guiding functional information systems to OSD Assistant Secretaries;
- redirected ongoing CIM programs to comply with the principles outlined by the ELG.

Lesson #3: There are lessons to be learned from the Executive Level Group. Get help from trustworthy, experienced professionals who do not have a vested interest in the outcome of what you want to do. If you want to innovate, do not accept conventional organizational boundaries. To get anything important done, demonstrate that by giving it the visibility, top management access and attention. Pick leaders who had already done what you wish to do.

Redirection - From Grand Design to Migration Systems

Even the best plans can be ruined by faulty execution.

The ongoing CIM effort violated just about every ELG principle. The first task for the new CIM regime would be to wipe out, with little salvage value, whatever had been invested in CIM for a period of two years. Although the official birth of CIM dated back to September of 1989, the ensuing turmoil of moving money and people meant that CIM, as we know it today, would not get started until the beginning of the next fiscal year, in October 1991.

I arrived on the job in March, 1991. A new manager has only a few weeks, and sometimes only a few days, to signal how his approach differs from the order he will replace. I had to pick where to drive my first stake. It had to be strategic. It had to assert a key ELG principle. It had to redirect people who were marching to a discredited tune. It had to satisfy an unfilled need.

To survive increasingly impatient Congressional staffs, CIM had to show that it could cut costs. CIM had been designated as the custodian as well as an investor for managing about a billion dollars per year that Congress had withdrawn for two years in succession from the Services and Agencies. CIM had to demonstrate that it was profitable. The problem was that the two-year old CIM was running out of Congressional patience.

The ELG principles dictated that without business measure of performance we could not succeed. However, CIM had been marching to the wrong measures of performance. Its orientation was to cut information technology costs, as reported to OMB. What is reported as "IRM" expenses, under the Brooks Act, is an irrelevant measure. For years I had lectured and written why the measure of Information Resource Management should not be computers, but information-related costs, as understood by business people. I decided to make a stand on the measures of performance.

In the second week in the Pentagon, the Institute of Defense Analysis made available to me Dr. Tom Frazier. He would help to put into place the *Functional Economic Analysis* [FEA method for evaluating IRM investments. Within two weeks Tom delivered the first version of the FEA software which is now one of the pillars on which all CIM is built. The basic premise of FEA is that what matters is risk-adjusted discounted functional cash flow, regardless of organizational boundaries. We have now done hundreds of FEA's. We found that the overwhelming source of savings is in functional costs, such as in administrative manpower, in inventories, in transportation and so forth. In one case the information technology cost figures is less than 4% of the discounted cash flow, although early delivery of a new application is critical in realizing the other 96% of benefits.

The introduction of the concept of FEA was traumatic and in many respects shattering to the IRM traditional views. The information technologists who were running CIM were now told to take a business view and maximize cash benefits that would directly support Mr. Cheney's and Mr. Atwood's $71.1 billion DMRD cost reduction target. Meanwhile, a large collection of governmental and self-appointed inspectors engaged us in discussions whether CIM was already a failure. As the measure of CIM accomplishments they always used year-to-year reductions in expenditures, as reported to OMB. In the ensuing exchanges I maintained that according to FEA principles CIM should be evaluated on how well it supported DMRD's. In a relatively short order the FEA point of view prevailed. The doubts about the financial viability of CIM were suspended by Congressional staffs, OMB, GAO, the press, industry associations, OSD onlookers and the Inspector General, at least temporarily.

FEA had a profound effect on how people started viewing systems development. Almost in every case, and that number is now over 1,000 major applications out of a total population estimated at 10,000, building a brand new system is the least desirable alternative. Selecting one of many redundant applications as the *Migration Application* and junking the rest is always preferable. One of the CIM "bumper stickers" says: *Reuse before you Build, Buy before You Build*. Reuse combined with selection of the best of the breed leads to an immediate generation of cash. It eliminates maintenance and operating expenses. The greatest benefits are, however, functional. Picking the best *Migration Application* and then enhancing it for universal use simplifies training, reduces data errors and begins the journey towards ultimate standardization of business processes.

The adoption of a policy of "applications triage" which will most likely eliminate over 9,000 existing "legacy" applications in the "back office" is now well established. This direction has

been advanced by Dr. Michael Mestrovich, who now maintains a directory of how and when various "legacy" applications are scheduled for extinction.

There is, however, life after a cluster of "legacy" applications are merged into one or two successor applications. At that point the CIM policies call for the introduction of the *Business Process Improvement* [BPI] method which means simplification, simplification and simplification before any automation takes place. It is only after the BPI is done, that CIM legitimizes discussions about client servers, integrated data-bases, distributed systems and what have you.

To motivate the existing organizations to engage in migration, the *Golden Nugget Award* emerged as the symbol that CIM was receptive to recognize the best that the Department had available, regardless of origin. It is good politics not to destroy organizations that surround you. You are a servant of the organization of which you are a part. Organizations have a culture, and you cannot go counter to that culture without punishment. You cannot use information technology to counteract the mental set of the people who will have to live with it. You can influence it somewhat, but you cannot overcome it. The best and surest way to reform an organization is to build innovations on top of the best that already exists. Every organization, regardless of how despondent, has somewhere a source of excellence. Every organization will somehow manage to nurture a few isolated pockets of homegrown competence. They are usually tucked away where the central bureaucracy does not reach, such as in Alaska, where I found a gusher of system innovations.

It is one of the CIM practices to nurture and leverage all seeds of excellence because they are a genuine source of proven experience. Hidden accomplishments usually grow from efforts that have flourished despite every conceivable obstacle. The rogue system, that everybody loves but that does not get official endorsement, demonstrates that excellence can grow on a minuscule budget if you have just a few talented and stubborn innovators. From CIM central funds we financed a modest level of small-scale home-grown initiatives. CIM refused to outsource all innovation to consultants. We had to build a Defense core capability to manage innovation. If you outsource everything you will find that there is nobody left to manage a new technology when it is finally ready for general use.

Lesson #4: There are lessons to be learned from the redirecting of systems designs from "grand" designs to *Migration Systems*. Prove yourself by first solving a significant problem. Link programs to recognized targets and objectives. Broaden the scope and definition of what system work is all about. Win commitment by helping people to learn how to apply new tools and how to discover new horizons. Make new tools. Emulate and reward excellence. Always count cash.

The Framework, Part I- Creating Policies

Institutions survive because of laws.

I joined the Department of Defense as a limited term executive. From the moment of its rebirth in 1991 CIM would be always running against a deadline that it would have to cease to be a temporary "initiative" and become a survivable permanent institution. CIM would become a

success only if its innovations become an accepted tradition. This meant getting out permanent directives, instructions and guidelines. These had to be drafted, coordinated, approved and issued. The closest analogy to DoD policy work is if you need a dentist's root canal job. It is necessary for continued good health, has to be done right, takes too long and is too expensive, is unpleasant and once done is hard to remove. Without well embedded policies, training in how to apply them and tools that make it easy to use them systems innovations do not survive their originators. The CIM program has produced an exemplary array of information management policy innovations which are now too deeply rooted to be easily extricated. These policies are well written - some are actually in legible English - thanks to Mr. Harry Pontius and the master OSD policy tactician, Mr. Ron Knecht. Most of these policies have generic applicability to any enterprise, and deserve to be copied, since good policy writing is rare. Here are some of the key policies that are shaping the future of CIM:

- **The Defense Information Management Program.** Defines scope, principles and organizational relationships. The grand charter of everything CIM stands for.
- **Defense Information Management Policies & Procedures.** Defines the "due process" for communicating about how to plan and implement information systems.
- **Life-Cycle Management of Automated Information Systems.** Defines the control and oversight process, while it emphasizes evolutionary and incremental development.
- **Functional Process Improvement.** Includes a Manual of how to do it. In terms of scope and long range impact, perhaps the most profound contribution of CIM. Inspired and guided by Mr. Michael Yoemans, one of the key contributors to CIM accomplishments.
- **Data Administration.** Includes a Manual of how to do it. The charter for the most ambitious data administration program ever conceived. The key to systems integration and interoperability. Without data administration there is chaos.
- **Functional Economic Analysis.** The policy that links information management to the business.
- **Technical Architecture Framework.** A five volume compilation to guide standard systems development. Includes an all important Technical Reference Model which specifies approved standards for development and acquisition.
- **Graphic Interface Style Guide.** Provides instructions what computer screens should look like to minimize training costs and errors.

Lesson #5: There are lessons to be learned from placing in effect a comprehensive array of CIM policies. Policies survive individuals. Making it a policy is the only means for assuring the institutionalization of innovation. Getting policy issued from the highest level of authority legitimizes implementation tactics. Policy to an innovator is like air cover and artillery support to the warfighter - bravery is insufficient when under fire.

The Framework, Part II- Creating Technology Directions

All civilization depends on its infrastructure. Only savages are self-sufficient.

Whenever I am engaged as a consultant, I start my education by first studying the evidence about systems failures. There is more substantive and relevant information in detailed descriptions of failed incidents than in any other conceivable source. The corollary to this observation is that a fancy slide presentation from the management is hardly ever of much use. With that bias established, I ordered a full set of *Government Accounting Office* [GAO] reports for five years. GAO is supposed to uncover failures. Thousands of pages of a litany about aborts, over-runs, breakdowns and contradictions conveyed a hard-to-believe record of persistent incompetence. If CIM was to fix any of that, it would require changing practices which were systemic and common to most incidents of failure. CIM could not and should not engage in trying to put out hundreds of fires.

The fundamental flaw shared by all Defense systems – something common to every GAO report – originates in the acquisition process. The acquisition practices enforce an approach that view each major new application as a separate, discrete and independent event. Defense has thousands of applications. With minor recent exceptions, each of them were built with a unique technology solution, under a unique contract, mostly with unique data formats, often with unique communications networks, with hardly any integration with related applications, applying in each case unique software methods and requiring an operating support environment that reflects the peculiarities of each acquisition incident. In mid 1992 I obtained a business flow diagram which describes every step in this process. That was easy to do because there are ten thousands of pages of procedures and regulations which tell a program manager exactly what forms to fill out to proceed from one check point to another. The systems acquisition diagram calls for completing over 5,000 events, in a rigidly prescribed sequence. No wonder it takes 5-10 years and multiples of $100 million dollars to deliver anything of value. Only a small fraction of the process is dictated by what needs to be done to fill a customer's needs. The overwhelming majority of the process deals with making sure that the unique technology solution can be validated, measured and tested.

The ELG concluded early in its deliberations that the acquisition of the difficult and long-lead time elements of systems must be independent of the application development effort. Separate the difficult "how" from the relatively easy "what". That means: provide a standard communications network; provide standard data elements that would be common to all applications; make available standard graphic interfaces for applications to minimize training; create a high level "integration" capability within Defense; require the use of standard business process models and systems engineering tools. In other words, provide the technology infrastructure as a generic fee-for-service commodity so that the acquisition process can concentrate on what is unique. The technology infrastructure would buy and provide generic hardware, software and communications services. Customers would have the tools to take care of their specific needs. Centralize the infrastructure so that you can truly decentralize services. The acquisition of the infrastructure and of the customer-owned assets would be separate. That would allow for incremental growth instead of engaging in giant, decade long acquisitions. The

objective should be for the customer to have the capability to add new fully tested functions to an already existing application for less than $10 million, in less than six months. All technical programs that have been launched under CIM have the acceleration and the cost reduction of applications as their unifying theme. The major CIM methodology programs are as follows:

- **Activity and Data Modeling.** CIM has institutionalized the IDEF method and was instrumental in launching it as a FIPS standard. I consider this effort the single most successful CIM venture investment. Acquired as a *Golden Nugget.*
- **Data Administration.** Development and operation of the DoD data repository. A key CIM strategic asset. Acquired as a *Golden Nugget.*
- **Activity Based Costing.** Although this enormously effective tool could be seen as CIM poaching on the Comptroller's grounds, we had to make the investment in this method in order to start automating the systems planning and engineering process.
- **Technical Integration Management [TIM].** Instituted the development of an overall technical architecture, configuration control and the management of cross-functional interfaces. This effort is an absolute requirement for assuring enterprise-wide interoperability of systems and data.
- **Technical Reference Architecture.** Guides the evolution of applications towards "open systems".
- **Enterprise Architecture.** This is the Holy Grail of all systems people. Advanced systems text books tell you that every organization must have one. Several CIM program Directors have attempted to come up with this abstraction, only to fail. Only someone with a depth of understanding about how the Pentagon really works can aspire to come up with anything that will be of use. Ms. Mary Smith has made the first breakthrough in this quest and is proceeding to test this construct.
- **Software Reuse Program.** Development and operation of the DoD software repository. Another CIM strategic asset. Acquired as a Golden Nugget. Much progress in this area is due to the leadership of Dr. Kurt Fischer.
- **Software Assessment and Improvement Program.** Adopts and administers the software maturity evaluation program.
- **Integrated Computer-Aided Software Engineering.** Provides all development organizations with standard software engineering tools and related training and technical services. Essential for achieving massive reductions in software costs. Another CIM strategic asset.
- **Information Technology Reuse Services [ITRUS].** Provides a streamlined hardware acquisition process and should extend the useful technology life of equipment. Another CIM strategic asset. Acquired as a Golden Nugget.
- **Defense Information Technology Services Organization [DITSO].** This organization was created as a pilot to test, evaluate and build a world-class information management organization within DISA. Managed with superb competence by Mr. Clyde Jeffcoat. DITSO is now a well established and proven operation and illustrates that even the public sector can operate information services entrepreneurially.

Lesson #6: There are lessons to be learned from launching a wide array of technology programs. You cannot chase every conceivable technology development. Almost all technology

should be provided by the commercial sector and certainly not developed internally. Concentrate on creating core competencies. Establish viable organizations. Develop skilled managers of information technology innovations. Acquire a cadre of experienced experts. Make sure that the technology programs share a unifying strategic direction, with measurable goals instead of standing as isolated explorations.

The Framework, Part III- Creating the Infrastructure

Defense capability first, cost reduction second.

Early in 1992 it became apparent that the Service guided consolidations would not deliver sufficient savings to support rising projections of Defense cutbacks. The total cash savings of the Service-managed consolidations would yield only a net $1.3 billions in savings by 1997, or less than 8% of the seven-year total cost baseline. What would be a more realistic productivity gain target? What would be the right benchmark against which to compare the seriousness of DoD efforts?

Industry results in unit cost reductions of data services are well documented. During the last decade the computer industry delivered staggering declines in the costs of information technologies. To skillful operators this has yielded enormous opportunities to reduce costs. The following is a record of productivity gains achieved by commercial firms in terms equivalent to the DoD seven-year planning cycle:

• Xerox	-81%
• Texas Instruments	-54%
• J.C.Penney	-76%
• EDS-Champus	-73%
• EDS-Eligibility	-42%
• EDS-Batch Update	-74%
• EDS-Batch Reports	-69%
• Karastan-Bigelow	-61%
• EDP Analyzer Report	-62%
• GTE	-75%
• Peat, Marwick	-65%

Clearly, something was amiss. The opportunities for cost reductions in Defense would be even greater. First, Defense would be starting from an already excessive cost base that has not been consistently cost managed. For instance, a consultant's comparison of the cost per MIP of some of the best DoD data centers showed that current costs were at least ten times greater than industry average. Second, operators such as Xerox and Texas Instruments scored their reported gains on top of an already long string or prior cost reductions. Third, DoD would be downsizing and its total volume of transactions would be cut back anyway. Unless the ongoing consolidation effort would make technology choices that cut fixed costs, after Defense downsizing the actual transaction cost by 1997 would be going up. Unfortunately, the services' consolidation plans were primarily driven by their mainframe orientation. After achieving their goals, their fixed costs would be up relative to future volumes.

The other difficulty with the services-managed consolidation concerned the base line against which savings would be made. If the annual baseline for achieving the productivity target was only about $2 billion, would changing the scope increase the chances of a higher payoff? It is a well known phenomenon in cost reduction studies that cost reduction opportunities increase faster when the scope of the effort is widened.

To resolve these questions was the task of DMRD 918. The analytic effort for this study was launched in May 1992. The first public draft of this DMRD suggested that the proper baseline for examining the productivity of information systems was much larger than was usually reported as the level of expenditures. This large number had already a number of exclusions in the absence of any progress in applying CIM methods in the excluded areas. The savings potential would be an order of magnitude greater than what services had committed to in their consolidations.

The DMRD 918 effort also provided the impetus to make an overall non-financial assessment of the conditions of the Defense information systems that excluded C^3I. The following are highlights of previously known characteristics:

1,000+ Data Processing Installations

- Average age over 11.5 years.
- 80% of capacity substantially below economic levels.
- Labor-intensive. Insufficient automation. Average costs per MIPS [Million instructions per second] greater than in industry, by a large multiplier.
- Do not share workloads and cannot act as back-up to each other.

38 Major Central Design Organizations. Staff of 6,000

- Engaged mostly in maintenance of obsolete code. Excessive development time.
- Non-standard development practices result in maintenance delays.
- Low levels of software capabilities. Local personnel takes maintenance into own hands.
- Inadequate technical and managerial experience to develop integrated applications.
- Applications reflect past contract award practices and therefore not compatible.
- Applications and data not interoperable or readily interchangeable.
- No standardization in data definitions and formats, which increases errors and costs.

650,000+ Workstations and Terminals

- Growth chaotic and costly. Electronic message exchanges limited to selected nets.
- No interoperability in document, graphic or picture formats.
- A large proportion of the total information resource management manpower engaged in developing applications meeting local needs.
- No software configuration control. High training and support costs.

102 Long Distance Networks

- Constructed to support traffic for specific organizations, applications or contracts.
- Costly lack of interoperability which requires reliance on liaison personnel.
- Labor intensive because no investments made in central monitoring and control.
- Poor capacity utilization because of fractured acquisition and old technologies.

10,000+ Local Area Networks

- Supports local preferences and locally improvised acquisition choices.
- Not interoperable. Excessive dependency on local small contractors.
- Exceedingly high support and maintenance costs.

The existing systems were not rapidly deployable, interoperable or secure. Their operating and maintenance costs were excessive as compared with what is commercially available. There was no committed plan to integrate and reduce the costs of C^3I applications. Yet, the quality of C^3I support would have to be the ultimate test whether CIM enhanced the US defense capabilities.

As the Corporate Systems Manager I concluded that a massive modernization was in order. In fact, without modernization Defense could not achieve the much needed cost reductions. The new defense infrastructure would have to provide for automatic linking between business, command, control, intelligence and communications functions. I also concluded that the financing of the required modernization investments would not require additional investments beyond the current funding levels. The necessary cash could be generated from swift cost-reductions in the current unreasonably high operating and maintenance expenses. If the pace of implementation could be speeded up, the modernization program could deliver the required capabilities while at the same time producing substantial net cash savings after the fourth year.

As the DMRD 918 evolved, I became increasingly apprehensive that during the next budget cycle, without a total commitment to an evolutionary modernization program, the available investment funds would be sacrificed to protect ten thousands of isolated computer adaptations that have sprung up from local initiatives. In the absence of a unified and generally accepted migration plan the prospects were dim. Without a broadly based and widely supported modernization efforts there was a chance that savings would be taken while the present infrastructure would only receive only the most urgent fixes. The money that would have been available for modernization would be then frittered away in maintaining an obsolete plant.

The arguments in favor of a modernization commitment were listened to, but not heard. Political realities have overtaken the events. DMRD 918, currently in implementation, has a much smaller baseline against which to make savings than initially proposed. The net savings are only 5.4% of the baseline. Its investment contents are very small relative to what is needed to support a concerted modernization program. DMRD 918 is a step in the right direction, but falls far short of being a significant strategic commitment to making information technology a distinct source of "competitive superiority". I am convinced that information superiority is perhaps the most cost-effective means for assuring the continued superiority of US arms in any warfare scenario of the future. DMRD 918 does not deliver that capability yet.

Lesson #7: There are lessons to be learned from an attempt to form a corporate infrastructure. They are similar to those noted in connection with the CIM start-up attempts. Financial goals are necessary, but certainly not sufficient. Policy and doctrine must always lead before information efficiency comes to play. Financial incentives and technology plans only work after top executives reach an agreement on concept of operations and how to change the management processes to reflect the new realities.

CIM Tasks Ahead - Education and Training

People come ahead of computers.

The Department of Defense cannot ever hope to achieve modernization of its information infrastructure without first enhancing the capabilities of its large information workforce:

Civilians	73,163
Active Duty Officers	18,386
Active Duty Enlisted	151,964
Active Military Total	170,350
Reserve Component Officers	11,103
Reserve Component Enlisted	114,827
Reserve Military Total	125,930
Total Information Systems	369,443

Mrs. Miriam Browning has completed a highly competent study which made an assessment of our educational and training needs. At present, the human resource development and planning is inadequate, by any standards. The urgent actions outlined in DMRD 918 with regard to training and education should not be delayed and should be seen as deserving top priority, ahead of more visible technology moves.

CIM Tasks Ahead - CALS and Outsourcing

Information Costs also Include the Costs of your Suppliers

Mr. Deane Erwin keeps telling me every month that DoD does not have integrated weapons databases. Weapon systems integrate applications, but only one at a time. The results are excessive administrative costs not only within DoD but also by contractors and subcontractors. So what should CALS [*Computer-Aided Acquisition and Logistics Support System*] executives do? They should examine the overall economics of acquisition and logistics transaction costs. This cannot be done by trying to sell individual solutions. The penalties for excessive transaction costs are in the gaps that exist between separate applications and in the pits that lie between administrative fiefdoms. CALS must first establish a top-down approach that deals with the economics of the entire chain of supply. Only after that should DoD approach it from a bottoms up direction and examine the validity of computer solutions.

In positioning CALS as a thrust that supports US Defense strategies DoD must look at aggregates that are larger than a weapon, a department, or a function. It must examine how to link to the industrial base and how to establish interoperability between industry and Defense. An examination of the events that connect all the elements from creation to distribution of information must start with understanding of the commercial environment that supports CALS. DoD must look at the commercial infrastructure and its costs, see how it interacts with Defens

and identify what is the damage to US competitive effectiveness because of Defense acquisition practices. CALS should adopt, as a governing principle, that it must maximize the use of the existing commercial infrastructure. Most defense contractors engage in commercial work. They must cope with global commercial adversaries and therefore must learn how to survive under conditions where business processes cannot tolerate excessive transaction costs. Therefore, the technology that is already in the hands of the commercial infrastructure is the technology that ought to drive CALS practices and standards. CALS should limit internal processing requirements to only those unique elements where commercial practices may violate the capabilities, security and readiness of our armed forces. CALS should also retain a capability to be an integrator "of last resort" of commercial systems elements.

There is one special point I would like to add about CALS software. I do not believe that DoD ought to spend money on developing completely unique CALS software. DoD must be able to integrate CALS systems for interoperability. DoD should concentrate its resources on taking care of only its unique needs, such as security and survivability. There is a flourishing commercial software industry, in the competitive market place, which is more nimble, more responsive, and more tested by the countervailing forces. The urgent need for the modernization of defense systems does not allow the luxury of arduous bidding processes, with very long and elongated delivery schedules and life cycle costs that are a large multiple of best industrial practice.

CALS executives should commit to a strategy that mandates commercial software products for DoD solutions. Software elements are now available in the market place that deliver equivalent CALS functionality as currently specified for defense uses. Private sector manufacturers now require standard data base products anyway. DoD executives should push for speed and reliability of inter-enterprise communications, rather than for automating the existing complexities of DoD's administrative processes.

This means that we will have to shift the responsibility for the development and operation of integrated weapons databases from the military departments to the US. industry. Otherwise DoD will incur horrendous costs of duplication of effort. Given the expected limitation of funds, Defense cannot afford any more the bifurcation of the information sector of the economy between the military the commercial sectors. Henceforth, the military and the commercial information sectors are nearly the same, except perhaps in the weapons areas. They are interdependent except in very limited areas. DoD should have every incentive to choose commercial services as the engine that supports universal needs. DoD should also see that there is a viable and low cost transaction services industry, so that military contracts to not impose on small firms large fixed costs.

CIM Tasks Ahead - Inclusion of C3 Planning

The Customer has Precedence over the Back Office.

C3 systems are by far the most costly components of Defense Information management. In operational terms they are all that matters, since all of the "IRM" systems must perform strictly

in a supporting role. It is therefore a major challenge for DoD to find how to plan, develop and manage C3I systems as integrated and interoperable elements. The policy on what is required is clear. Gen. Colin Powell, in the *C2 Functional Analysis and Consolidation Review Panel Report* of November 25, 1992 endorsed the following principles also echoed in DMRD 918:

- The needs of small, mobile and locally managed forces shall receive high priority for post-Cold-war information systems.
- The concept of the *Defense Information Infrastructure* [DII] is to transfer to a global infrastructure centralized support functions for difficult and costly systems elements, such as communications network management, software configuration control and data administration.
- The objective of the DII is to provide small forces with the same or superior support capabilities as currently possessed by large commands, at a much lower cost.
- The DII approach to risk management shall address the low end of the conflict spectrum. Because the combat forces will be small, light and mobile, they will consist principally of combat personnel and equipment. Consequently systems management shall require minimal staff deployment in combat zones.
- The future low-intensity warfare forces will have to rely primarily on non-organic, rear-area or regional information systems support and the ready availability of a global infrastructure capable of supplying unit-tailored information.
- The systems of the future as seen as evolving from the current theater-centric and service-centric designs towards a global, Joint Defense Information Infrastructure that supports Joint Task Forces (JTF) or Combined Task Forces (CTF) as the primary operational objective.
- JTF's, rather than the component command headquarters become the principal operational command elements below unified commanders.
- Require a restructuring of DoD systems so that any Joint Tactical Command can manage their forces directly and immediately.

Given these policy guidelines, it would be reasonable to expect that the C3 community would embark on their implementation. That has not happened. A number of worthwhile "quick fix" projects are now proceeding, including a number supported by CIM funding and CIM methods, under the guidance of Mr. John Graves. Individual services are now starting to consider migration and consolidation plans, but within limits of each service. However, there is a large number of high-cost C3 systems which are neither interoperable nor unique. Therefore, C3 is the last functional area that remains the prime prospect for choosing migration paths which would follow the CIM method to streamline and simplify information systems. The size of the C3 information systems baseline makes it the most attractive prospect for cost reduction. In terms of modernization, a limited review of C3 systems suggests that a rapid introduction of modern and low cost technologies is even more urgent here than in the "back office" functions.

What would be the applications of CIM principles and practices to C3?

- With smaller, more diversified and unpredictable force deployments DoD shall foster information systems designs that transcend traditional Service and CINC boundaries through centrally managed systems support capabilities. That means

that an OSD master systems plan must be articulated before individual Services can proceed with their own streamlining efforts.

- Centralized management of application systems through lead agencies under Joint management, will be then essential to invest into modernization with reduced resources. That implies the need for a central planning and budgeting process for all systems development, similar to the ones that have been adopted by other OSD functions.
- The development, acquisition, testing and evaluation processes for enterprise and mission-level Joint information systems will be under the direction of the Defense Information Systems Agency. This implies a large scale reassignment of program management responsibilities from Services to DISA.
- The objective of a Joint C3 systems architecture would be to build into all information systems long-life (20+ years) modularity, interoperability and flexibility, from the start, as their central design principle. This is not presently the case, since each major Service program follows their unique technology development directions.
- Mandate that the design of all information systems be fully modular and inter-operable to fit into a wide range of force deployments. This implies central configuration control of hardware and software for the entire Defense Department.
- Require that the design of all information systems be assembled from standard components and inter-operable to instantly construct a unique command and control structure. This principle is the big money saver and performance enhancer for C3. It would require instilling a much stronger discipline over contractors that now develop software without regard to any global reuse.
- Proceed with development of information systems designs that would favor a more centralized and consolidated design approach while increasing systems survivability through redundancy of facilities at widely dispersed points of geography. What it means is that we will have to start designing systems to cope with rapid new trends in information-based warfare.
- Provide complete information systems interoperability with automatic data processing and office automation applications for seamless inquiries concerning, personnel, medical, financial, materials, logistics and transportation data. That interoperability now exists only painfully and slowly. To comply with this principle would require the conformity of all C3I applications to the CIM *Enterprise* and *Mission* models.
- Set up central Functional Integration Organizations, at the Enterprise, Mission and Functional levels following CIM guidelines and methods throughout C3.

Bringing C3 information systems planning into the forefront of all CIM strategies is then the largest and single most important opportunity for further progress.

Summing Up

CIM should never become a proxy for territorial contentions between OSD, Services and Agencies. Some of the debates that I've attended concerning DMRD 918 looked more like meetings of the United Nations about Bosnia, where everybody subscribes to general

pronouncements except that nobody wishes to commit to anything that would alter existing arrangements in any major way. CIM participants must lift themselves from the ongoing debates about localized interests. Strengthening a Federation to achieve a greater unity of purpose need not necessarily diminish local capabilities. The basic premise of CIM was that its objective is to manage the hard-to-do infrastructure. In this way local commanders can be freed to satisfy their immediate needs, quickly, easily and inexpensively. The declared objective of CIM was to move over 90% of all computing capabilities directly into the hands of local commanders.

If we don't work together and lower DoD's information management costs, somebody else will do it by drastic means that will degrade US warfare capabilities. Bureaucratic privileges, contractual privileges, or regulatory precedence should take a secondary place to making Joint warfighting capabilities the basis for further CIM progress. CIM is not a zero-sum-game, where every change means that there are losers. The condition of the existing DoD information infrastructure is so bad that with cooperation everybody should be a gainer.

Without commitment to a major modernization of the current information management structure there is only a limited future for CIM. It may degrade to become the means for achieving localized cost reductions. The CIM program, or its successor acronym, has the capability of supporting the development of US information superiority. This is perhaps the most cost-effective means for assuring the continued superiority of US arms in any warfare scenario of the future. That is the promise, that is the potential: Information Superiority for Defense Superiority.

Thank you for this opportunity to share with you what I have learned in two most wonderful years of my entire professional career. It was a privilege to serve the Defense of the United States as it learns to cope with information-based warfare of the future.